

## **INSTRUMENTOS GPS Y PODER DE CONTROL DEL EMPRESARIO**

**Daniel Pérez del Prado**

Investigador en formación. Becario FPU  
Área de Derecho del Trabajo y de la Seguridad Social  
Universidad Carlos III de Madrid

### **PALABRAS CLAVE**

Poder de a la intimidad, derecho a la protección de datos de carácter personal.

### **RESUMEN**

La utilización de las nuevas tecnologías tiene importantes repercusiones en las relaciones laborales y, en particular, en lo que hace al equilibrio entre el poder de dirección y control del empresario (art. 38 CE) y los derechos fundamentales inespecíficos de los trabajadores. El presente artículo, aborda la concreta incidencia que los dispositivos de localización denominados comúnmente como “GPS” están teniendo en el ámbito laboral, así como cuál está siendo su tratamiento jurisprudencial.

\* \* \*

### **SUMARIO**

**I. Introducción. II. Los antecedentes: la videovigilancia. III. La protección de datos de carácter personal. Deslinde con el derecho a la intimidad y respuesta de la Agencia Española de Protección d Datos. IV. Tratamiento judicial de la utilización de dispositivos GPS para vigilancia y control en el ámbito laboral. V. Algunas reflexiones finals. VI. Bibliografía.**

## I. Introducción

Las relaciones entre los derechos fundamentales de los trabajadores y los poderes del empresario resultan una materia ya clásica en el ámbito del Derecho del trabajo. En efecto, numerosas han sido las ocasiones en que nuestros tribunales se han tenido que enfrentar a la resolución de casos en los que se ha denunciado un uso ilegítimo de los poderes con que cuenta el empresario para la dirección de la empresa, muy especialmente los poderes de control y disciplinario, lo cual devenía en una lesión de los derechos fundamentales del trabajador, ya se trate de los específicamente reconocidos como tales por la Constitución como tales, esto es, derechos de huelga y libertad sindical; ya sean cualesquiera otros derechos fundamentales que alcanzan una especial configuración cuando se manifiestan en el ámbito laboral<sup>1</sup>.

Sin embargo, se trata éste de un campo poco estable, sujeto, quizá, no a numerosas variaciones en lo que hace a su regulación por parte del Derecho, pero sí en lo que respecta a la aparición de numerosos avances tecnológicos que plantean nuevas cuestiones, nuevos casos, nuevos conflictos.

Porque, en efecto, la aparición de nuevos ingenios tecnológicos puede suponer, y de hecho supone, una mejora de las condiciones de trabajo y, en su caso, un incremento de la productividad de la empresa. Sin embargo, su utilización como mecanismo de control de la actividad de los trabajadores por parte del empresario, además de plantear importantes dilemas morales<sup>2</sup>, nos presenta también relevantes retos jurídicos. No es que el empresario tenga que renunciar a sus derechos (art. 38 CE) ante los del trabajador (art. 35 CE). De lo que se trata es que los avances tecnológicos no lleven la dirección y control

---

<sup>1</sup> Para una visión general de los llamados derechos fundamentales inespecíficos, *vid.* PALOMEQUE LÓPEZ, M. C., *Derechos Fundamentales Generales y Relación Laboral: los Derechos Laborales Inespecíficos*, en SEMPERE NAVARRO (DIR.), *El Modelo Social en la Constitución Española de 1978*, MTAS, Madrid, 2003, págs. 229-248.

<sup>2</sup> Para un ejemplo de los pros y contras del mecanismo tecnológico a que se refiere el presente estudio, *vid.* MICHAEL, K.; MCNAMEE, A.; MICHAEL, M. G., "The Emerging Ethics of Humancentric GPS Tracking and Monitoring", *Working Paper*, 2006.

del empresario a tal extremo que la empresa se convierta en una suerte de “fábrica panóptica”, en la que el trabajador está totalmente controlado en todo lo que hace<sup>3</sup>, una especie de nuevo «feudalismo industrial», que «tanto repugnan al Estado social<sup>4</sup>».

En efecto, más allá de los aspectos positivos que los avances tecnológicos pueden suponer no sólo para la empresa sino para el propio desenvolvimiento de la actividad laboral, no cabe duda de que existen también elementos negativos. En el presente trabajo, nos referiremos a uno en concreto, esto es, a su incidencia en los derechos a la intimidad y a la protección de datos. Sin embargo, existen algunos otros como son los riesgos psicosociales<sup>5</sup> asociados al trabajo y que se conectan directamente con ese control absoluto de la “fábrica panóptica” a que hacíamos referencia.

Por otra parte, uno de los últimos avances incorporados al mundo del control de los trabajadores ha sido precisamente el de los Dispositivos de Posicionamiento Global, más conocidos por sus siglas en inglés, GPS<sup>6</sup> (*Global Positioning System*). Se trata de un sistema de localización, diseñado por el Departamento de Defensa de los Estados Unidos, con fines militares, para proporcionar estimaciones precisas de posición, velocidad y tiempo.

El sistema se compone de tres segmentos básicos, los dos primeros

---

<sup>3</sup>La referencia está tomada de MERCADER UGUINA, J.R., *Derecho del trabajo. Nuevas tecnologías y sociedad de la información*, Editorial Lex Nova, Valladolid, 2002, págs. 99-101. En las páginas siguientes el autor aborda el modo en que los avances tecnológicos chocan con el disfrute de los derechos fundamentales del trabajador y la forma en que la jurisprudencia ha venido resolviendo tales conflictos. Así, se refiere a supuestos tales como la videovigilancia, la vigilancia microfónica, las etiquetas electrónicas y las tarjetas inteligentes u otras relacionadas con el ámbito de las telecomunicaciones. A este respecto, *vid.* págs. 101-124. Sobre la relación entre control empresarial y nuevas tecnologías, también puede consultarse GOÑI SEIN, J. L., “Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos”, *Justicia Laboral. Revista de Derecho del Trabajo y de la Seguridad Social*, nº 39, 2009, págs. 11-58.

<sup>4</sup> STC 88/1985 de 19 de julio, FJ 2.

<sup>5</sup> LANDSBERGIS, P., “¿Qué se debe hacer para prevenir los riesgos psicosociales en el trabajo?”, *Archivos de prevención de riesgos laborales*, vol. 11, Nº 1, 2008.

<sup>6</sup> Cuando el dispositivo GPS se encuentra acoplado a un terminal telefónico móvil se denomina GMS (Global System Mobiles), aunque en el presente trabajo utilizaremos la denominación genérica “GPS”.

de responsabilidad militar: el llamado “segmento espacio”, formado por 24 satélites; el “segmento control”, que consta de cinco estaciones monitoras encargadas de mantener en órbita los satélites y supervisar su correcto funcionamiento, tres antenas terrestres que envían a los satélites las señales que deben transmitir y una estación experta de supervisión de todas las operaciones; y el “segmento usuario”, formado por las antenas y los receptores pasivos situados en tierra. Los receptores, a partir de los mensajes que provienen de cada satélite visible, calculan distancias y proporcionan una estimación de posición y tiempo<sup>7</sup>.

La actividad de estos satélites y receptores permite, como es de sobra conocido, calcular no sólo la posición de cualquier objeto en la tierra, sino observar su movimiento o calcular las distancias que recorre o pretende recorrer. Así, su aplicación práctica en el ámbito civil ha alcanzado en los últimos años un amplísimo desarrollo: navegación aérea, terrestre y marítima; aplicaciones agrarias e industriales; investigaciones geológicas y geodésicas; etc.<sup>8</sup> Tal ha sido su éxito, que la Unión Europea está desarrollando su propio proyecto conocido con el nombre de “Galileo”.

Pues bien, como ya se ha señalado, la utilización del GPS no ha escapado, como es obvio, al ámbito de las relaciones laborales. En efecto, el GPS se ha convertido en un instrumento muy útil en actividades como el transporte terrestre, marítimo o aéreo, entre otros, pero también un instrumento eficaz para que el empresario pueda conocer cómo están siendo utilizados los materiales puestos a disposición del trabajador y, lo que resulta más controvertido, dónde se encuentra éste en cada momento.

Aunque, como ya hemos adelantado, nos vamos a referir a un concreto ámbito de la incidencia de la utilización de los dispositivos GPS en las relaciones laborales, existen muchas otras, algunas de carácter negativo. Así, en el ámbito de los mencionados riesgos psicosociales, por citar un ejemplo, se ha impuesto la intervención del Derecho para hacer frente al estrés en el traba-

---

<sup>7</sup> EL-RABBANY, A., *Introduction to GPS: the Global Positioning System*, Artech House, 2006, págs. 1-11.

<sup>8</sup> *Ibid*, págs. 129-151.

jo causado por el seguimiento electrónico constante de la ubicación de los trabajadores en el desempeño de sus funciones o, incluso, durante sus horas de descanso.

En el concreto ámbito que estudiamos, la negociación colectiva ha debido intervenir para imponer límites y frenar los excesos. En los Estados Unidos, por ejemplo, en un centro de llamadas en Arizona, el Sindicato de Trabajadores de las Comunicaciones de América y la AT&T eliminaron las mediciones individuales y el seguimiento secreto. Por lo que respecta al dispositivo objeto de nuestro estudio, el GPS, de manera similar, en una compañía Chicago, los empleados urbanos se negaron a utilizar móviles con GPS y obtuvieron el derecho a apagar los móviles durante los descansos y después del trabajo. De forma similar, el sindicato de transportistas acordó con la compañía “UPS” que se utilizara el GPS sólo para hacer un seguimiento de los envíos y no para controlar disciplinariamente a los trabajadores<sup>9</sup>.

A lo largo de las próximas páginas veremos cuál ha sido la respuesta que el Derecho ha ofrecido para permitir la utilización de esta nueva tecnología en correcta comunión con la garantía y respecto de los derechos fundamentales del trabajador.

## II. Los antecedentes: la videovigilancia

Quizá el antecedente más claro al caso que vamos a tratar en el presente estudio se encuentre en la videovigilancia. En efecto, se trata de una técnica de control de los empleados que se desarrolla normalmente en el seno de la empresa y que permite, no solamente controlar en cada momento dónde están, como es el caso del GPS, sino, además, saber qué están haciendo. Cuando la actividad a que se refiere la empresa traspasa los muros de la misma, esto es, cuando la naturaleza de la actividad laboral exige su desempeño

---

<sup>9</sup> LANDSBERGIS, P., “¿Qué se debe hacer para prevenir los riesgos psicosociales en el trabajo?”, cit., pág. 41.

fuera de un habitáculo cerrado, como es el caso de los transportistas, conductores de ambulancias, transporte de viajeros, etc. se impone la necesidad, no tanto de saber qué hace en ese pequeño habitáculo, sino de controlar a dónde se dirige con él y los fines con que se utiliza el patrimonio empresarial.

Por consiguiente, el seguimiento GPS puede verse como una forma evolucionada de videovigilancia para aquellos casos en que la actividad desempeñada por el trabajador es móvil, por lo que no importa tanto lo que hace la mayor parte del tiempo, sino si utiliza los instrumentos y bienes de la empresa para el fin para el que le fueron entregados. De ahí que sea interesante dedicar algunas líneas al tratamiento jurídico de esta otra tecnología.

Además, como veremos, la utilización de dispositivos GPS guarda una intrínseca relación con el derecho a la intimidad (aunque no será el único derecho en juego), el cual precisamente se pone en entredicho cuando de la utilización de la videovigilancia se trata.

En efecto, el tratamiento jurídico de la videovigilancia supone la ponderación, de una parte, del derecho a la intimidad de los trabajadores; de otra, del poder de organización y control empresarial. Como veremos también en el caso del GPS, de tal ponderación resulta, no la exclusión de alguno de los dos, sino la articulación de la forma de su convivencia. Así, el ordenamiento jurídico no prohíbe la instalación de cualquier aparato televisivo que sirva para el control del trabajo pero, a su vez, establece una serie de limitaciones, de tal forma que no resulta válida ni justificada cualquier uso o cualquier emplazamiento. Como señala el profesor MERCADER, «en suma, la instalación de videocámaras por el empresario para el control de la actividad de los trabajadores y de los lugares de trabajo es legal, aunque tiene determinados límites: el primero, directamente derivado del art. 20 ET, es el respeto a la dignidad del trabajador, si bien este derecho no puede considerarse violado por el mero hecho de la instalación de videocámaras<sup>10</sup>»

---

<sup>10</sup> MERCADER UGUINA, J.R., *Derecho del trabajo. Nuevas tecnologías y sociedad de la información*, cit., pág. 102.

A este respecto, el Tribunal Constitucional ha establecido una regla general sobre la que articular el juego entre los derechos de ambos polos de la relación jurídica. Tal regla general no es otra que el principio de proporcionalidad, en virtud del cual, cabe concluir la constitucionalidad de cualquier medida restrictiva de derechos fundamentales siempre que resulte “proporcionada”. Pero, ¿en qué consiste el canon interpretativo de la proporcionalidad?

Podemos tomar como ejemplo la STC 66/1995 que, para un supuesto relativo al derecho de reunión, lo definía del siguiente modo: «para comprobar si la medida impeditiva del ejercicio del derecho (...) supera el juicio de proporcionalidad exigible, es necesario constatar si cumple los siguientes tres requisitos o condiciones: si tal medida era susceptible de conseguir el objetivo propuesto (...); si, además, era necesaria en el sentido de que no existía otra medida más moderada para la consecución de tal propósito con igual eficacia, y, finalmente, si la misma era proporcionada, en sentido estricto, es decir, ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto<sup>11</sup>». Por consiguiente, decir que una medida es proporcionada y que, por tanto, no lesiona derechos fundamentales supone superar un triple juicio, esto es, el juicio de idoneidad o que la medida sea susceptible de conseguir el objetivo propuesto; el juicio de indispensabilidad o estricta idoneidad, es decir, que no exista otra medida más moderada para la consecución de tal fin; y, por último, el juicio de proporcionalidad en sentido estricto, que supone que la medida sea equilibrada, derivándose de ella más beneficios que perjuicios.

Pues bien, esta doctrina fue precisamente aplicada por el Tribunal Constitucional en un supuesto de videovigilancia. Se trata de la STC 186/2000, que resuelve un supuesto de instalación de cámaras de videovigilancia en un economato. En concreto, la empresa, al observar un descuadre entre los rendimientos de dos de sus secciones, decide instalar un circuito cerrado de televisión que, sin conocimiento de los trabajadores, enfocase únicamente a las tres cajas registradoras y al mostrador de paso de mercancías. Las imágenes ofrecidas por este medio, sirvieron de base para el despido de uno de los trabajadores.

---

<sup>11</sup> STC 66/1995, de 8 de mayo, FJ 5.

Así las cosas, y refiriéndonos únicamente a aquellos aspectos de las sentencia relevantes para este apartado, la Sala comienza señalando que «el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho»

Precisamente uno de esos límites es el constituido por el poder de dirección del empresario «imprescindible para la buena marcha de la organización productiva (organización que refleja otros derechos reconocidos constitucionalmente en los arts. 33 y 38 CE) y reconocido expresamente en el art. 20 LET», que atribuye a éste, entre otras facultades, la de adoptar las medidas que estime más oportunas para la vigilancia y el control del cumplimiento, por parte del trabajador, de sus obligaciones laborales. A lo que añade «mas esa facultad ha de producirse en todo caso, como es lógico, dentro del debido respeto a la dignidad del trabajador, como expresamente nos lo recuerda igualmente la normativa laboral<sup>12</sup>».

Por consiguiente, el empresario no queda apoderado para llevar a cabo, al amparo de las facultades de vigilancia y control que le confiere el art. 20.3 LET, intromisiones ilegítimas en la intimidad de sus empleados. Se trata, como ya quedó dicho, de ponderar el derecho a la intimidad del trabajador con el poder de dirección y control del empresario. Como señala el propio Tribunal constitucional, «los equilibrios y limitaciones recíprocos que se derivan para ambas partes del contrato de trabajo suponen, por lo que ahora interesa, que también las facultades organizativas empresariales se encuentran limitadas por los derechos fundamentales del trabajador, quedando obligado el empleador a respetar aquéllos<sup>13</sup>».

Tal ponderación supone, en definitiva, aplicar el principio de proporcionalidad para, de esta forma, determinar si utilización de cámaras de video

---

<sup>12</sup> STC 186/2000, de 10 de julio, FJ. 5.

<sup>13</sup> STC 292/1993, de 18 de octubre, FJ 4.



por parte del empresario constituye una intromisión ilegítima o no en el derecho a la intimidad del trabajador.

Pues bien, del razonamiento seguido por la sentencia se va a deducir que la medida que se llevó a cabo, esto es, la instalación de un circuito cerrado de televisión que controlaba la zona donde los trabajadores desempeñaban su actividad laboral, era una acción que no lesionaba el derecho a la intimidad y, ello, porque era una medida justificada (ya que existían razonables sospechas de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo); idónea para la finalidad pretendida por la empresa (verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja y a una duración temporal limitada, la suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada).

En efecto, a juicio del Tribunal, la intimidad del recurrente no resultaba agredida por el mero hecho de filmar cómo desempeñaba las tareas encomendadas en su puesto de trabajo, pues esa medida no resulta arbitraria ni caprichosa, ni se pretendía con la misma divulgar su conducta, sino que se trataba de obtener un conocimiento de cuál era su comportamiento laboral, ante las sospechas de que se podía estar realizando graves irregularidades, constitutivas de transgresión a la buena fe contractual. Como advierte la propia Sentencia, «se trataba, en suma, de verificar las fundadas sospechas de la empresa sobre la torticera conducta del trabajador, sospechas que efectivamente resultaron corroboradas por las grabaciones videográficas, y de tener una prueba fehaciente de la comisión de tales hechos, para el caso de que el trabajador impugnase, como así lo hizo, la sanción de despido disciplinario que la empresa le impuso por tales hechos<sup>14</sup>».

Por último, la Sentencia aún realiza un par de puntualizaciones que pueden resultar interesantes. En primer lugar, distingue el supuesto que resuelve de otro planteado con anterioridad, el de la STC 98/2000. En el caso

---

<sup>14</sup> STC 186/2000, FJ. 7.

que estamos estudiando la medida no obedeció al propósito de vigilar y controlar genéricamente el cumplimiento por los trabajadores de las obligaciones que les incumben, a diferencia del anterior. En aquél, la empresa, un casino, existiendo un sistema de grabación de imágenes, pretendía añadir un sistema de grabación de sonido para “mayor seguridad”, sin que quedara acreditado que este nuevo sistema se instalase como consecuencia de la detección de una quiebra en los sistemas de seguridad ya existentes y tal medida resultase indispensable para la seguridad y buen funcionamiento del casino.

En segundo lugar, resta importancia al hecho de que la instalación del circuito cerrado de televisión no fuera previamente puesta en conocimiento del Comité de empresa y de los trabajadores afectados, sin duda, advierte «por el justificado temor de la empresa de que el conocimiento de la existencia del sistema de filmación frustraría la finalidad apetecida», para a continuación señalar que «carece de trascendencia desde la perspectiva constitucional, pues, fuese o no exigible el informe previo del Comité de empresa a la luz del art. 64.1.3 d) LET, estaríamos en todo caso ante una cuestión de mera legalidad ordinaria, ajena por completo al objeto del recurso de amparo. Todo ello sin perjuicio de dejar constancia de que los órganos judiciales han dado una respuesta negativa a esta cuestión, respuesta que no cabe tildar de arbitraria o irrazonable, lo que veda en cualquier caso su revisión en esta sede».

Esto último, debe ser subrayado ya que, como veremos, el elemento de la información resulta imprescindible para que la medida pueda ser considerada como legal y, nos atreveríamos a señalar, como no vulneradora de derechos fundamentales, por más que en el caso estudiado el Tribunal Constitucional no le otorgara importancia.

Sea como fuere, la respuesta contenida en la Sentencia puede generalizarse de tal forma que la videovigilancia o cualquier otra medida de control basada en las nuevas tecnologías serán respetuosas con los derechos fundamentales de los trabajadores en el ámbito laboral siempre que resulten proporcionadas, esto es, siempre que resulten idóneas, indispensables y equilibradas.

No obstante, a propósito de este canon de enjuiciamiento, autores como GOÑI ponen de manifiesto un cierto deterioro del mismo en su aplicación

judicial, que lleva a que «esté siendo aplicado por los jueces y tribunales ordinarios pero con resultados no siempre satisfactorios, porque lo que se está poniendo de manifiesto es que no en pocas ocasiones la aplicación es un tanto superflua y, a la postre, más formal que real<sup>15</sup>».

De ahí que el juicio de proporcionalidad le resulte, en general, insuficiente, a la vez que advierte que no atiende los problemas derivados de la vulneración del derecho del trabajador sobre sus datos de carácter personal. «Este principio se detiene en una simple consideración de los límites a la actividad de indagación del empresario; no atiende más allá de los peligros provenientes de la intrusión sobre la conducta de la persona del trabajador. Y no comporta directriz alguna sobre los límites a la posibilidad del empresario de tratamiento de las informaciones recabadas en las actividades de control ni sobre los derechos del trabajador frente a los riesgos de manipulación y utilización de esas informaciones<sup>16</sup>».

### **III. La protección de datos de carácter personal. Deslinde con el Derecho a la intimidad y respuesta de la Agencia Española de Protección de Datos**

Una de las variantes del derecho fundamental inespecífico de a la intimidad es el concerniente a la protección de los datos de carácter personal<sup>17</sup>. De la lectura de los arts. 1 y 3 de la LOPD se puede deducir fácilmente que su objeto es la garantía y protección de los datos personales, entendiendo por

---

<sup>15</sup> GOÑI SEIN, J. L., “Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos”, cit., pág. 17.

<sup>16</sup> *Ibid*, pág. 19.

<sup>17</sup> Esta conexión se establece expresamente en el art. 1 de la LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante LOPD), que transpone a nuestro ordenamiento la Directiva 95/46. En el mismo sentido se ha pronunciado el Tribunal Constitucional en su STC 292/2000, de 30 de noviembre, FJ 2.

tales «cualquier información concerniente a personas físicas identificadas o identificables».

Su importancia en la sociedad de nuestros días es vital y su comprensión permite un redimensionamiento y actualización de otros derechos fundamentales clásicos y, en particular, el derecho a la intimidad, tanto en su versión genérica (art. 18.1 CE), como en la específica relacionada con los medios informáticos (apartado cuarto del mismo precepto). En palabras del propio Tribunal Constitucional «la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada “libertad informática” es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención<sup>18</sup>»

No obstante, a pesar de su evidente relación con algunos de los derechos que componen el haz que integra el art. 18 CE, el Tribunal Constitucional se encargó de deslindarlos convenientemente al señalar que «este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran<sup>19</sup>».

---

<sup>18</sup> SSTC 11/1998, de 13 de enero, FJ 5; y 94/1998, de 4 de mayo, FJ 4

<sup>19</sup> STC 292/2000, de 30 de noviembre, FJ 5, aunque también dedica el siguiente a la mencionada distinción.

Todo ello llevó a nuestro Alto Tribunal a afirmar la especialidad diferenciada de la protección de datos de carácter personal, que definió como «un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso<sup>20</sup>.»

Pues bien, esta definición, unida a la legal de la LOPD antes transcrita, nos permite entender que lo que se protege y garantiza es la disposición y control de cualquier dato o información, siempre que sea concerniente a una persona física o jurídica. Por consiguiente, no tiene por qué tratarse de datos íntimos, ni relativos a la vida privada de las personas a que se refieren, ni que gocen de un especial carácter confidencial.

Y, de ahí, la conexión con el objeto del presente estudio. En efecto, los dispositivos GPS no proporcionan datos íntimos ni confidenciales, pero sí datos protegibles de acuerdo con lo previsto en la LOPD, en tanto que identificativos de la posición geográfica de un determinado sujeto, en este caso el trabajador, a lo largo del tiempo.

Por consiguiente, cualquier empleador que sea consciente de la necesidad de respetar tales datos de carácter personal se enfrentará a la siguiente pregunta: ¿qué hacer con los datos proporcionados por el GPS?

A esta pregunta responde precisamente la Agencia Española de Protección de Datos en su informe 193/2008. En su contestación a la consulta formulada, la agencia distingue dos momentos temporales distintos:

- a) Momento previo a la utilización del dispositivo GPS como mecanismo de control. A este respecto recuerda que, aunque el art. 20.3 del ET dispone que «el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el

---

<sup>20</sup> STC 292/2000, de 30 de noviembre, FJ 7.

trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso», y que, por tanto, el empresario goza de legitimación legal para adoptar este tipo de medidas en general, y mediante la utilización del dispositivo GPS, en particular. Sin embargo, tal autorización legal no excluye el cumplimiento de su deber de informar, previsto en el artículo 5.1 de la LOPD.

Así las cosas, la utilización de un dispositivo GPS para el ejercicio de las facultades de control del empresario requiere que el trabajador conozca, previamente a su uso, que va a ser sometido a este control tecnológico, esto es, debe ser previamente informado de modo expreso, preciso e inequívoco de su seguimiento y, en particular de: i) la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; ii) el carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; iii) las consecuencias derivadas de la obtención de los datos o de la negativa a suministrarlos; iv) la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y v) la identidad y dirección del responsable del tratamiento.

- b) Tratamiento de los datos obtenidos con el GPS. Cumplidos los anteriores requisitos legales el empresario estará facultado para utilizar el dispositivo GPS como instrumento de control de la actividad de sus trabajadores. No obstante, sus responsabilidades no terminan allí. En efecto, tal y como señala el informe, la utilización de esta tecnología y la emisión de datos de carácter personal que de la misma se derivan, imponen al empleador todo un catálogo de obligaciones de recogida, tratamiento, uso, almacenamiento y cesión que, de no ser cumplidos, pueden conllevar al lesión del mencionado derecho y, de ahí, la responsabilidad de este.

Así las cosas, la consulta consideraba responsable de estas obligaciones a la empresa consultante, conclusión que podría extenderse a la generalidad de los casos y que se basa en la definición prevista

por el artículo 3 d) de la LOPD<sup>21</sup>, desarrollada por el Real Decreto 1720/2007, de 21 de diciembre, en el artículo 5.1 q)<sup>22</sup>.

Tal sujeto responsable estará obligado, en primer lugar, a la inscripción de los datos de carácter personal en el Registro General de Protección de Datos. Para proceder a la inscripción de un fichero en el Registro, se debe cumplimentar el modelo establecido en la Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, (BOE N° 181, de 31 de julio de 2006), por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático.

Así, este formulario electrónico de Notificaciones Telemáticas permite la presentación de notificaciones a través de Internet (con y sin certificado de firma electrónica reconocido), mediante soporte informático (disquete, CDROM) y en soporte papel, encontrándose disponible en la página web de la Agencia ([www.agpd.es](http://www.agpd.es)).

En definitiva, la protección de datos de carácter personal conlleva dos tipos de obligaciones esenciales, una *ex ante* de información, otra *ex post*, de tratamiento de los mismos. La relevancia de estos dos grandes núcleos o bloques se pone de manifiesto en las diversas ocasiones en que la Agencia de Protección de Datos se ha tenido que pronunciar, como consecuencia de la apertura de expedientes sobre denuncias sobre supuestas vulneraciones del derecho a la protección de datos de resultados de la utilización de dispositivos GPS. Tal es el caso de la Resolución del Director de la Agencia de Protección de Datos de 17 de julio de 2007 (Expediente N° E/00587/2006), en que se acuerda el archivo de las actuaciones, tras comprobar que la empleadora, en

---

<sup>21</sup> «La persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento»

<sup>22</sup> «Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente».

este caso, un Administración pública, había obrado correctamente en lo que hace a las dos obligaciones mencionadas. En efecto, se trata de un caso en el que un conductor, tras la apertura de un expediente sancionador sobre la base de los datos obtenidos por el GPS, alega que su empleadora «dispone de ficheros no inscritos en el Registro General de Protección de Datos, en los que se recogen datos de carácter personal relativos a control de horarios del personal que presta servicios en la misma, un registro histórico de los conductores de vehículos oficiales y datos proporcionados por el sistema “GPS” instalados en dichos vehículos, tales como situación del vehículo, velocidad, tiempo de parada o de funcionamiento. A este respecto, denuncia que dichos datos se han obtenido sin el conocimiento ni el consentimiento de las personas que utilizan los vehículos».

Ante los datos aportados, la Agencia entiende que no se ha producido vulneración por cuanto los trabajadores fueron previamente avisados de la utilización de tales dispositivos y hubo un tratamiento e inscripción adecuados de los ficheros contenedores datos de carácter personal<sup>23</sup>.

#### **IV.Tratamiento judicial de la utilización de dispositivos GPS para vigilancia y control en el ámbito laboral**

Son ya numerosas las sentencias que versan sobre la utilización de dispositivos GPS en el ámbito laboral cuando su utilización resulta una cuestión

---

<sup>23</sup> GOÑI critica esta resolución por entender que de ella se desprende un criterio de control de la injerencia patronal sobre la intimidad del trabajador caracterizado por su excesiva automaticidad, permitiendo casi cualquier tipo de actuación por parte del empresario siempre que preavise y sin tener en cuenta ni el principio de finalidad legítima del art. 4 LOPD ni el de transparencia. GOÑI SEIN, J. L., “Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos”, cit., págs. 23-26. Por otra parte, haciendo referencia especial a la primera de las obligaciones, a la de información a los trabajadores, y conteniendo diversas vías en que puede procederse a cumplir con dicha obligación, puede consultarse también el Expediente N°: E/00742/2008.



adyacente o colateral, una mera forma de prueba<sup>24</sup>; pero muy pocas aún aquellas en el que el tema objeto de nuestro estudio constituye una alegación de fondo o principal. En relación con esto último, conviene advertir que, lógicamente, nos estamos refiriendo a casos en los que el recurrente alega vulneración de su derecho a la intimidad (art. 18 CE) con carácter general, o en su versión específica relativa a la protección de datos de carácter personal. Al objeto del presente trabajo, haremos referencia a dos que nos han resultado especialmente significativas.

En primer lugar, la STSJ del País Vasco, de 2 de julio de 2007<sup>25</sup>, se refiere, en su fundamento jurídico segundo, a una supuesta vulneración del derecho a la intimidad como consecuencia de la utilización de un dispositivo GPS incorporado al teléfono móvil de la empresa, cuyos datos se utilizaron, junto a otros indicios, para despedir al trabajador. En concreto, se trata de un supuesto de despido disciplinario de un escolta, que firmando un parte como que había realizado un determinado servicio, en realidad no lo hizo, lo que tras oportuno expediente, acabó con la extinción de la relación laboral.

Pues bien, la primera alegación del recurso es precisamente, como ya quedó dicho, una supuesta vulneración del derecho a la intimidad sobre la base de lo dispuesto en los arts. 18.1 CE y 4.2 e) y 18 ET. En concreto, el demandante que tal vulneración se produce como consecuencia de que «la empresa ha obtenido la prueba de que no hizo el servicio el día de autos mediante un sistema de localización GPS del teléfono móvil que tenía asignado, desconociendo los trabajadores de la empresa esta circunstancia del mismo».

---

<sup>24</sup> Con frecuencia, los datos recogidos válidamente por los dispositivos GPS suelen utilizarse como prueba para la imposición de una sanción y, por lo que aquí respecta, para la más grave de ellas, que es el despido. Este es el caso de la STSJ de Madrid 1185/2004, de 28 diciembre; la STSJ de Galicia 3736/2008, de 17 de octubre; STSJ de Andalucía 1724/2007, de 20 de junio; STSJ de Castilla-La Mancha 922/2009, de 28 de mayo; STSJ de Galicia 1845/2009, de 7 abril; STSJ de Madrid. 679/2006 de 19 de septiembre; STSJ de La Rioja 299/2006, de 26 septiembre; STSJ de Galicia 4930/2005, de 23 noviembre; STSJ de Galicia 3345/2008, de 19 septiembre; STSJ de Madrid 510/2008, de 3 junio; STSJ de Asturias 1652/2009, de 22 mayo; STSJ de Galicia 1845/2009, de 7 abril; STSJ de Cataluña 6515/2008, de 1 de septiembre; STSJ de Galicia 3080/2005, de 13 julio; STSJ de Cataluña 5089/2005, de 2 junio; STSJ de Madrid 233/2003, de 18 marzo, STSJ de Madrid 10/2009, de 12 enero.

<sup>25</sup> Número de Recurso 1175/2007.

Antes que nada debe subrayarse que, a pesar de lo que hemos señalado anteriormente sobre las relaciones entre el derecho a la intimidad y a la protección de datos, el demandante utiliza exclusivamente aquél. Sin duda que esto se debe a la especial protección de que goza como consecuencia de su consagración constitucional. Sin embargo, como también se vio, esto no habría obstado (recuérdese que la protección de datos de carácter personal goza también de esa protección de forma derivada, como especie de aquel género), para intentar lograr una protección más específica a través de la regulación especial ofrecida por la LOPD. Así las cosas, de los datos ofrecidos por la sentencia, no llega a comprenderse por qué se utiliza la vía genérica, sin el apoyo de la específica; si por desconocimiento, al tratarse de una materia relativamente novedosa o, por el contrario, si ello no se hizo por motivos prácticos, estratégicos o de imposibilidad fáctica.

Sea como fuere, el caso es que el Tribunal rechaza la existencia de vulneración sobre la base de dos motivos: por una parte, porque no se presenta prueba alguna de tal vulneración; por otra, que no fueron los datos del GPS, los verdaderamente tenidos en cuenta por el órgano *a quo* a la hora de determinar la validez del despido.

En relación con el primero, resulta útil reproducir parte de la argumentación utilizada por el Tribunal: «claro es que este otro tipo de despido también es nulo si concurre alguna de esas circunstancias (art. 55 .5 ET y art. 108.2 LPL), siendo uno de los derechos fundamentales del trabajador el de intimidad personal que nuestra Constitución reconoce en su art. 18.1 y del que no queda privado en el ámbito de la relación laboral (art. 4.2 e ET), que desde luego queda afectado si el empresario utiliza un sistema de control del trabajo de sus empleados que se desarrolla fuera de sus dependencias a través de un sistema de localización permanente del teléfono móvil que se facilita como instrumento de trabajo, sin consentimiento ni conocimiento de aquéllos, máxime si éstos han de tenerlo a su disposición en todo momento por estar sujetos a disponibilidad permanente, ya que si bien resulta un medio idóneo para controlar su labor (de lo que no le priva que pueda hacerse un uso que le impida realizar esa función, como sucede si el teléfono en cuestión no lo lleva consigo el trabajador), en modo alguno resulta necesario si tenemos en cuenta que el propio sistema de telefonía móvil siempre permite conocer ese dato y, por tanto, ac-

ceder a ese conocimiento con autorización judicial si concurren circunstancias que justifican una actuación de esa naturaleza, tan invasora del campo propio de la intimidad personal. Esfera, ésta, que ni tan siquiera desaparece durante la jornada laboral, en la que el trabajador mantiene un reducto en el que su empresario no puede penetrar si no resulta preciso por exigencias de la relación laboral, mediante un medio idóneo, necesario y suficientemente proporcionado al sacrificio de ese derecho fundamental».

De estas afirmaciones cabe deducir varios elementos importantes. En primer lugar, el Tribunal tampoco se aparta del género para acercarse a la especie, como le permite el principio *iura novit curia*, máxime en el ámbito de los derechos fundamentales; no obstante, es plenamente consciente de la necesidad de conocimiento y consentimiento para que las prácticas invasivas de la intimidad del trabajador y, en particular, el seguimiento mediante GPS, sea legal, esto es, respete el mencionado derecho; en tercer lugar, sin embargo, no entra a dilucidar si existió conocimiento o no y si esto se realizó conforme a lo dispuesto en la ley, sino que se limita a afirmar el mecanismo de control vía GPS «en modo alguno resulta necesario si tenemos en cuenta que el propio sistema de telefonía móvil siempre permite conocer ese dato y, por tanto, acceder a ese conocimiento con autorización judicial si concurren circunstancias que justifican una actuación de esa naturaleza, tan invasora del campo propio de la intimidad persona». En relación con esto, debemos decir que, aunque fuera cierto, aunque pudiera averiguarse la ubicación exacta del trabajador únicamente con el teléfono móvil, más allá de los datos ofrecidos por éste relativos a su uso únicamente profesional o no, lo interesante jurídicamente hablando es precisamente que los datos ofrecidos por el GPS se obtienen sin autorización judicial, sin las garantías que esto supone. Esto abre la puerta al estudio jurisprudencial acerca de la legalidad de la forma de su obtención, así como su utilización como prueba en juicio; puerta que en este caso el Tribunal no abre.

Es cierto, como vamos a analizar a continuación, y como bien señala la Sala, que tales alegaciones no se realizaron por el cauce procesal adecuado, ni revistieron en su enjuiciamiento ante el órgano *a quo* la suficiente entidad como haber entrado a conocer del asunto, pero nada impedía en la referencia a la regulación del derecho a la intimidad en conexión con la utilización de nuevas

tecnologías, haber hecho una referencia expresa al concreto aspecto del derecho sobre los datos de carácter personal, que es lo que verdaderamente se alegaba.

Dicho esto, tiene razón el Tribunal cuando, en relación a lo anterior, señala que «no estamos ante un simple defecto formal del recurso, ya que en el desarrollo del motivo no se invoca prueba documental o pericial que avale la realidad del hecho alegado (como lo exige el art. 191 b) LPL si se quiere revisar la versión judicial de los hechos acaecidos), limitándose a señalar que no puede darse credibilidad a los testigos que intervinieron, como tampoco al representante de la empresa cuando, en su interrogatorio, reconoció haber informado de ello al comité de empresa».

En efecto, aunque la sentencia no lo ponga de manifiesto expresamente no hace a este respecto sino aplicar la doctrina constitucional sobre la inversión de la carga de la prueba en casos de supuesta vulneración de derechos fundamentales. Tal doctrina se sintetiza en la STC 17/2007, de 11 de febrero, al recordar que «cuando se prueba indiciariamente que una extinción contractual puede enmascarar una lesión de derechos fundamentales, este Tribunal ha reiterado, desde nuestra STC 38/1981, de 23 de noviembre, que incumbe al empresario acreditar que su decisión obedece a motivos razonables y ajenos a todo propósito atentatorio del derecho de que se trate. Para ello, es preciso que el trabajador aporte un indicio razonable de que el acto empresarial lesiona su derecho fundamental, principio de prueba o prueba verosímil dirigido a poner de manifiesto el motivo oculto que se denuncia y que debe permitir deducir la posibilidad de que ha podido producirse. Sólo una vez cumplido este primer e inexcusable deber, recaerá sobre la parte demandada la carga de probar que su actuación tuvo causas reales absolutamente extrañas a la pretendida vulneración, así como que tenían entidad suficiente para justificar la decisión adoptada (por todas, reproduciendo esa doctrina, SSTC 29/2002, de 11 de febrero, FJ. 5; 30/2002, de 11 de febrero, FJ. 3; 17/2003, de 30 de enero, FJ. 4; y 342/2006, de 11 de diciembre, FJ. 4)<sup>26</sup>»

---

<sup>26</sup> STC 17/2007, de 11 de febrero, FJ 4.

Por consiguiente, para que opere la inversión de la carga de la prueba, que hubiera obligado a la empresa a demostrar que no hubo intromisión en el derecho a la intimidad (ni vulneración de los datos de carácter personal), se imponía la necesidad de cumplir con el primero de los requisitos, esto es, aportar un indicio razonable de tal vulneración, cosa que el demandante no logra. Así, de la lectura del apartado C de este fundamento jurídico segundo que venimos analizando, no se desprende que lo alegado por el recurrente llegue a construir un “indicio razonable”, sino todo lo más, ciertas alegaciones que el juzgado extrajo por la vía de la presunción judicial, pero que no constituyen indicio suficiente.

El resto de la sentencia se refiere a cuestiones ajenas al objeto del presente estudio.

Por último, también reviste cierto interés, aunque sea sólo porque el objeto del conflicto, la STSJ de Madrid 679/2006, de 19 septiembre. En ella no se discute acerca de la vulneración del derecho a la intimidad o a la protección de datos de carácter personal del actor, sino que se trata de un caso de supuesto boicot al aparato GPS.

En efecto, el caso a que se refiere la sentencia es el de un conductor de ambulancias que es despedido disciplinariamente como consecuencia de que el aparato GPS dejó de funcionar en diversas ocasiones, atribuyendo tal circunstancia a una manipulación por parte del trabajador. En concreto, de la sentencia del Juzgado de lo Social interesa destacar la siguiente información:

- a) La principal imputación contenida en la carta de despido se refiere a que el GPS incorporado a la ambulancia que habitualmente utilizaba el trabajador dejó de funcionar durante los dieciocho días en los períodos de tiempo debidamente concretados en la sentencia.
- b) Tal imputación fue considerada «prueba plena» sobre la base de dos tipos de probatoria: la documental, aportada por la empresa, consistente fundamentalmente en los partes-informes de incidencia y los datos informáticos del programa que controlaba

el estado del mencionado dispositivo; y la testifical. En relación con esta, se menciona, en primer lugar, la declaración del ex presidente del Comité de Empresa, que aseveró que la introducción y aceptación del referido sistema informático de control, fue acordado en reunión de la dirección y el Comité de Empresa. Así las cosas, y aunque nada se dice al respecto, debe advertirse que, tal y como quedó dicho, se hace necesario además el conocimiento por parte del trabajador, cosa que parece deducirse del relato y de la actitud que supuestamente se le imputa. En segundo lugar, también se menciona la declaración del informático de la empresa, encargado del control de los aparatos GPS, quien aclaró y especificó que realizó personalmente en dos ocasiones comprobaciones de dicho aparato en la propia ambulancia y que funcionaba con absoluta normalidad, siendo el único de los ciento cincuenta dispositivos que compondrían la flota que tuviese esas incidencias, por lo que sugirió “ponerle una pequeña trampa” consistente en el lacrado de uno de los cables, comprobándose posteriormente que dichos cables habían sido rotos.

Pues bien, sobre la base de lo anterior, el Sala procede a la resolución del caso, de forma muy escueta, en el fundamento jurídico segundo de la Sentencia. Así, en un primer momento, la Sala reprocha a la empresa que durante el período en que se detectaron los fallos en el funcionamiento del dispositivo GPS, sin que éstos pudieran atribuirse al propio aparato, debió procederse a sancionar al trabajador no consintiendo que este comportamiento lesivo y abusivo frente a la empresa «continuase produciendo durante el período indicado».

Posteriormente, se introduce en la cuestión en sí para advertir que «no consta que los días que se produjeron estos hechos, el servicio técnico revisase al principio y al final de la jornada laboral el sistema para comprobar que el mismo funcionaba correctamente». Es decir, tras comprobar que durante un período determinado de tiempo el aparato fallaba, fue cuando la empresa decide proceder a revisar de nuevo el sistema. Es entonces cuando precinta las conexiones del mismo al objeto de determinar si efectivamente este se está manipulando manualmente o si por el contrario pudiera deberse a la utilización

de un sistema electrónico de inhibición sin que conste que «ello se haya efectuado con las debidas garantías por el informático de la empresa»

Esa falta de garantías y de control de los precintos lleva a la Sala afirmar que no puede imputarse al trabajador su rotura «cuando previamente no se ha constatado sin ningún género de dudas y con las debidas garantías, el estado en que se encontraban los precintos». De ahí, la estimación el recurso interpuesto por el trabajador.

En cualquier caso, hemos querido traer aquí esta sentencia con el objeto de constatar que, ante las nuevas formas de control por parte del empresario, surgen también nuevas formas de boicot por parte de los trabajadores, boicot que puede suponer, de comprobarse un abuso de la buena fe y, en última instancia, algún género de sanción en función de su gravedad. En todo caso, como constata la sentencia, aún en tales casos, la garantía de los derechos de los trabajadores en el ámbito laboral, en este caso la presunción de inocencia, es un pilar fundamental sobre el que descansan las relaciones laborales en nuestro ordenamiento jurídico.

## **V. Algunas reflexiones finales**

A través del presente estudio hemos pretendido ofrecer un bosquejo del tratamiento legal y jurisprudencial que la utilización de dispositivos GPS tiene en un nuestro ordenamiento jurídico.

Así, nos hemos encontrado con dos derechos, el derecho a la intimidad y el derecho a la protección de datos de carácter personal, en principio, distintos, pero que la propia doctrina del Tribunal Constitucional califica como “afines”, por cuanto tienen como objetivo común ofrecer una eficaz protección constitucional de la vida privada personal y familiar. De ahí que pueda hablarse de una cierta especialidad, de un género y una especie.

También hemos visto que, a pesar de ciertas dudas que despierta su

aplicación, el canon jurisprudencial con que se cuenta para determinar si la utilización de dispositivos electrónicos por parte del empresario para controlar la actividad del trabajador es el principio de proporcionalidad. Sin embargo, las escasas sentencias que hasta ahora han tratado la utilización de dispositivos GPS como objeto principal del conflicto (sí son más numerosas aquellas que utilizan los datos obtenidos por estos aparatos como prueba para justificar las faltas del trabajador), no han tenido ocasión de aplicar este criterio, a pesar de que el derecho que se reclamaba como supuestamente vulnerado era precisamente el de la intimidad, lo que pone nuevamente de manifiesto la estrecha vinculación entre los apartados 1 y 4 del art. 18 CE a que acabamos de hacer referencia.

Por otra parte, del análisis de las resoluciones de la AEPD sobre los requisitos que han de cumplirse para el correcto tratamiento de los datos de carácter personal se desprende, ciertamente, una cierta automaticidad<sup>27</sup>. Posiblemente la misma deriva de la estanqueidad con que pretende tratarse el tratamiento de los datos de carácter personal respecto de del derecho a la intimidad, lo que justificaría las críticas a que también se hicieron referencia.

Es aquí donde, quizá, el principio de proporcionalidad, reformado o no, puede jugar un papel relevante como complemento a los criterios que la AEPD exige para entender como legal una determinada práctica de control basada, en nuestro caso, en dispositivos GPS. En efecto, los requisitos *ex ante* y *ex post* deberían acompañarse de un tercer requisito que atienda a la finalidad y justificación de la medida, lo cual tiene su apoyatura legal en el art. 4 LOPD. Tal requisito, se satisfaría observando si la acción es idónea, imprescindible y proporcionada, lo cual, de momento, no parece haberse tenido en cuenta en los criterios de aplicación de nuestra normativa sobre protección de datos de carácter personal.

De esta forma, se llegaría a conclusiones distintas y no cualquier actividad, sería susceptible de ser controlada vía GPS (quizá sólo aquellas en las el elemento “traslaticio” resulta esencial); ni en cualquier momento, lo que dejaría al margen, por ejemplo, los momentos de descanso del trabajador.

---

<sup>27</sup> Vid. nota 23.



En definitiva, parece que aún quedan diversas cuestiones por perfilar en este concreto campo, en el que, por otra parte, la jurisprudencia tiene aún mucho que decir.